CALIFORNIA
OFFICE OF
PRIVACY
PROTECTION

Recommended Practices on Notice of Security Breach Involving Personal Information

May 2008

October 2003
Rev. April 2006
Rev. February 2007
Rev. May 2008

California Office of Privacy Protection
www.privacy.ca.gov
866-785-9663

Contents

Introduction

Identity Theft

Identity theft has been called the crime of the 21st century, favored, according to law enforcement, for its low risk and high reward. Not only do identity theft victims sometimes have to spend money out of pocket to clear up their records, but they also must devote their time – up to hundreds of hours in some cases – to doing so. In the meantime, victims may be unjustly harassed by debt collectors, denied credit or employment opportunities; they may lose their cars or their homes, or be repeatedly arrested for crimes they did not commit.

According to the most recent nationwide survey, over eight million Americans were victims of identity theft in 2007. The same survey estimated the total cost of identity theft in the U.S. at $45 billion.[1]

Precisely how most identity theft occurs and the role of information security breaches is not clear. The major nationwide surveys have found that more than 60 percent of victims do not know how their personal information was acquired by a thief.[2] Consumers can often protect their personal information from some types of data theft, such as stolen mail or wallets and "phishing" emails. Other risks, however, are beyond consumer control. One academic study of identity theft cases found that in over half of the crimes, insiders in organizations were involved.[3]

In recent years, a particularly pernicious type of identity theft has been noticed. Medical identity theft occurs when someone uses an individual's name and sometimes other identifying information without the individual's knowledge to obtain medical services or products. Medical identity theft has been called the information crime that can kill you, because in addition to a financial dimension it can also result in putting dangerously inaccurate information in the victim's medical records. This form of identity theft can be very difficult to discover and to correct, and the procedures for responding to the more common forms of financial identity theft are not available in the medical arena.[4]

Information Security

Security has always been an essential component of information privacy. It is one of the basic principles of fair information practice: Organizations that collect or manage individuals' personal information should use security safeguards to protect that information against unauthorized access, use, disclosure, modification, or destruction.[5]

Implementing an effective information security program is essential for an organization to fulfill its responsibilities towards the individuals who entrust it with their personal information. It is the best way to reduce the risk of exposing individuals to the possibility of identity theft. It is also the best way to reduce the risk of an information security breach and the resultant cost to an organization's reputation and finances.

Many organizations in the United States are legally required to protect the security of personal information. The two major federal laws on privacy enacted in recent years - the Gramm-Leach-Bliley Act and the Health Insurance Portability and Accountability Act - include security regulations that apply to a broad range of financial services companies and health care organizations.[6] A California law also requires businesses to use reasonable and appropriate security measures to protect specified personal information of California residents.[7] Another California law imposes a similar requirement on state government agencies.[8]

Security Breach Notification

One of the most significant privacy laws in recent years is the California law intended to give individuals early warning when their personal information has fallen into the hands of an unauthorized person, so that they can take steps to protect themselves against identity theft or to mitigate the crime's impact. While the law originally focused on breaches involving the kind of information used in financial identity theft, growing concern about medical identity theft led to the addition of medical and health insurance information as "notice-triggering" in 2008.

Since the California law took effect in 2003, news reports of breaches have brought the issue of information security to public attention. Notifying affected individuals in such cases has become a standard practice, and at least 43 states have enacted notification laws based on California's.

The breach notice law has done more than give individuals notice. It has also resulted in improved privacy and security practices in many organizations. While the law does not require entities experiencing a breach to notify the California Office of Privacy Protection, many individuals, companies, and agencies have contacted the Office with questions about notification. In an effort to identify and spread best practices, the Office has studied these breach notifications and has synthesized many lessons learned from them.

One lesson is made clear by the significant share of breaches resulting from lost or stolen laptops and other portable devices, about 45 percent of the publicly known breaches.[9] Organizations have begun to pay more attention to protecting personal information on portable devices. Some organizations are doing this by using encryption. Others have adopted new procedures to safeguard the information, such as cabling PCs to desks, not allowing the downloading of Social Security numbers from mainframes onto PCs or laptops, and tightly restricting the number of people who are permitted to carry sensitive personal information on portable devices.

Another lesson is the ubiquity of Social Security numbers in databases and other records. Three quarters of the publicly known breaches involved Social Security numbers.[10] Individuals face the greatest risk of serious identity theft problems when their Social Security numbers fall into the wrong hands. Recovering from these types of identity theft can take hundreds of hours and thousands of dollars, making early discovery critical.

Some organizations that have experienced breaches of Social Security numbers have revised their data retention policies. After a breach that exposed 15-year-old data, a university reviewed its policies and decided to shorten the retention period for certain information, including Social Security numbers, on applicants who were not admitted.

Others have reconsidered their collection of the sensitive personal information in the first place. A blood bank which, like several others with mobile operations, had a laptop stolen, changed its policy of collecting Social Security numbers and decided to rely instead on the donor numbers that they were already using.

The California Office of Privacy Protection's Recommended Practices

California law obligates the Office of Privacy Protection to protect the privacy of individuals' personal information by "identifying consumer problems in the privacy area and facilitating [the] development of fair information practices."[11] One of the ways that the Office is directed to do this is by making "recommendations to organizations for privacy policies and practices that promote and protect the interests of California consumers."[12]

The recommendations offered here are neither regulations, nor mandates, nor legal opinions. Rather, they are a contribution to the development of "best practices" for businesses and other organizations to follow in managing personal information in ways that promote and protect individual privacy interests.

In developing the recommendations, the Office received consultation and advice from an advisory group made up of representatives of

the financial, health care, retail, technology and information industries, state government agencies, law enforcement, and consumer privacy advocates. When updating the recommendations to address medical information, additional advisors were consulted. A list of advisory group members can be found in Appendix 1. The group members' contributions were very helpful and are greatly appreciated.

Recommended Practices

The California Office of Privacy Protection's recommended practices are intended to assist organizations in supplementing their information privacy and security programs. The recommendations are not regulations and are not binding. Nor are they limited to the scope of the California law on notice of security breach, but rather they represent a broader approach and a higher standard.

These "best practices" recommendations can serve as guidelines for organizations, to assist them in providing timely and helpful information to individuals whose personal information has been compromised while in the organization's care. Unlike many best practices sets, however, these recommendations do not contain all the practices that should be observed. Information-handling practices and technology are changing rapidly, and organizations should continuously review and update their own situation to ensure compliance with the laws and principles of privacy protection. It is recognized that specific or unique considerations, including compliance with other laws, may make some of these practices inappropriate for some organizations.

Our practice recommendations are presented in three parts: Part 1 - Protection and Prevention, Part II - Preparation for Notification, and Part III - Notification. While the California law on notice of security breach applies to unencrypted "computerized data," we recommend applying these practices to records in any media, including paper records.

Definitions

The following are definitions of key terms used in these recommended practices. (Note that the bold terms are not used in the statute.)

Notice-triggering information: As provided in California law, this is unencrypted, computerized information, specifically first name or initial and last name plus any of the following:

- Social Security number,
- driver's license number or California Identification Card number,
- financial account number, in combination with any required code or password permitting access to an individual's financial account,
- medical information, as defined on pages 22-23 OR
- health insurance information, as defined on pages 22-23.

Data owner: The individual or organization with primary responsibility for determining the purpose and function of a record system.

Data custodian: The individual or organization that has responsibility delegated by the data owner for maintenance and technological management of the record system.

Data subject: An individual whose notice-triggering information is involved in a security breach.

Part I: Protection and Prevention

While an organization's information security program may be unique to its situation, there are recognized basic components of a comprehensive, multi-layered program to protect personal information from unauthorized access.[13] An organization should protect the confidentiality of personal information whether it pertains to customers, employees or others. For both paper and electronic records, these components include physical, technical and administrative safeguards. Among such safeguards are the following recommended practices.

1. Collect the minimum amount of personal information necessary to accomplish your business purposes, and retain it for the minimum time necessary.

- Identify your business reasons for collecting and retaining personal information, particularly notice-triggering information (Social Security numbers, driver's license or State ID numbers, financial account numbers, medical information, health insurance information).

2. Inventory records systems, critical computing systems, and storage media to identify those containing personal information.

- Include laptops and portable devices used to store personal information.

3. Classify personal information in records systems according to senstivity.

- Identify notice-triggering personal information.

4. Use appropriate physical and technological security safeguards to protect personal information, particularly notice-triggering information, in paper as well as electronic records.

- Authorize employees to have access to only the specific categories of personal information their job responsibilities require.
- Where possible, use technological means to restrict internal access to specific categories of personal information.
- Monitor employee access to higher-risk personal information.
- Remove access privileges of former employees and contractors immediately.

5. Pay particular attention to protecting notice-triggering personal information on laptops and other portable computers and storage devices.

- Restrict the number of people who are permitted to carry such information on portable devices.
- Consider procedures such as cabling PCs to desks or prohibiting the downloading of higher-risk personal information from servers onto PCs or laptops.
- Use encryption to protect personal information on portable computers and devices.[14]

6. Do not use data containing personal information in testing software or systems.

7. Promote awareness of security and privacy policies and procedures through ongoing employee training and communications.

- Monitor employee compliance with policies and procedures.
- Include all new, temporary, and contract employees in security and privacy training and monitoring.
- Impose penalties for violation of security and privacy policies and procedures.

8. Require service providers and business partners who handle personal information on behalf of your organization to follow your security policies and procedures.

- Make privacy and security obligations of third parties enforceable by contract.[15]
- Monitor and enforce third-party compliance with your privacy and security policies and procedures.

9. Use intrusion detection technology and procedures to ensure rapid detection of unauthorized access to higher-risk personal information.

- Conduct periodic penetration tests to determine effectiveness of systems and staff procedures in detecting and responding to security breaches.

10. Wherever feasible, use data encryption, in combination with host protection and access control, to protect higher-risk personal information.

- Data encryption should meet the National Institute of Standards and Technology's Advanced Encryption Standard.[16]

11. Dispose of records and equipment containing personal information in a secure manner.

- Shred paper records with a cross-cut shredder and use a program to "wipe" and overwrite the data on hard drives.[17]

12. Review your security plan at least annually or whenever there is a material change in business practices that may reasonably implicate the security of personal information.

- For example, if an organization decides to outsource functions that use personal information, such as using a call center, the plans should be revisited to take the new third parties into account.

13. If you are a health plan or health insurer, provide patients with regular explanation of benefits statements.

- Explanation of benefits statements should be sent promptly following every service or in response to patient request.
- Statements should be in plain, consumer-friendly language and should contain a contact number for patients to ask questions about the statements.

Part II: Preparation for Notification

An information security program should contain an incident response plan, which addresses security incidents including unauthorized access to or acquisition of higher-risk personal information.[18] To ensure timely notice to affected individuals, the following practices are among those that should be included in an incident response plan.

1. Adopt written procedures for internal notification of security incidents that may involve unauthorized access to higher-risk personal information.

2. Designate one individual as responsible for coordinating your internal notification procedures.

3. Regularly train employees, including all new, temporary and contract employees, in their roles and responsibilities in your incident response plan.

- Collect 24/7 contact numbers for incident response team and provide to team members.
- Make sure that all employees and contractors can recognize a potential breach and know where to report it.

4. Define key terms in your incident response plan and identify responsible individuals.

5. Plan for and use measures to contain, control and correct any security incident that may involve personal information.

6. Require the data custodian or others who detect an information security incident to immediately notify the data owner upon detection.

7. Identify appropriate law enforcement contacts to notify on security incidents that may involve illegal activities.

- Appropriate law enforcement agencies may include California's regional high-tech crimes task forces, the Federal Bureau of Investigation, the U.S. Secret Service, and the local police or sheriff's department. See Appendix 4 for contact information.

8. Consider suggestions from law enforcement with expertise in investigating high-technology crimes for inclusion in your incident response plan.[19]

9. If you plan to notify affected individuals by e-mail, get the individuals' prior consent to the use of e-mail for that purpose.

- See the consent procedures in the federal Electronic Signature Act.[20]

10. Adopt written procedures for notification of individuals whose unencrypted notice-triggering personal information has been, or is reasonably believed to have been, acquired by an unauthorized person.

- Include unauthorized acquisition of computer printouts and other paper records containing notice-triggering personal information in your notification procedures.

11. Document response actions taken on an incident. This will be useful to your organization and to law enforcement, if involved.

- At the conclusion of an incident, review events and actions and make any indicated changes in your technology and response plan.

12. Review your incident response plan at least annually or whenever there is a material change in your business practices.

- Update your breach response plan to address breaches of medical and health insurance information.

13. If you are a health plan or health insurer, be prepared to implement additional safeguards when member or subscriber information is compromised in a breach.

- If an individual reports that his or her health insurance policy number or subscriber identification number was used by someone else or was compromised in a breach, give the individual a new number, if feasible..
- Consider "flagging" compromised policy or subscriber numbers, if feasible, and using special procedures to verify identity of anyone requesting services under flagged numbers.

Part III: Notification

Openness or transparency is another basic privacy principle. An organization that collects or manages personal information should be open about its information policies and practices. This responsibility includes informing individuals about incidents such as security breaches that have

caused their unencrypted personal information to be acquired by unauthorized persons. The purpose of notifying individuals of such incidents is to enable them to take actions to protect themselves against, or mitigate the damage from, identity theft or other possible harm.

To ensure giving timely and helpful notice to affected individuals, the following practices are recommended.

Acquisition

In determining whether unencrypted notice-triggering information has been acquired, or is reasonably believed to have been acquired, by an unauthorized person, consider the following factors, among others:

1. Indications that the information is in the physical possession and control of an unauthorized person, such as a lost or stolen computer or other device containing unencrypted notice-triggering information.
2. Indications that the information has been downloaded or copied.
3. Indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported.

Timing of Notification

Notify affected individuals in the most expedient time possible after the discovery of an incident involving unauthorized access to notice-triggering information.

1. Take necessary steps to contain and control the systems affected by the breach and conduct a preliminary internal assessment of the scope of the breach.
2. Once you have determined that the information was, or is reasonably believed to have been, acquired by an unauthorized person, notify affected individuals within 10 business days.
    - Do this unless law enforcement authorities tell you that providing notice at that time would impede their investigation.

Contacting Law Enforcement

If you believe that the incident may involve illegal activities, report it to appropriate law enforcement agencies.

1. In contacting law enforcement, inform the law enforcement official in charge of the investigation that you intend to notify affected individuals within 10 business days.
2. If the law enforcement official in charge tells you that giving notice within that time period would impede the criminal investigation:
    - Ask the official to inform you as soon as you can notify the affected individuals without impeding the criminal investigation.
    - Be prepared to send the notices immediately upon being so informed.
    - It should not be necessary for a law enforcement agency to complete an investigation before notification can be given.

Whom to Notify

If your assessment leads you to reasonably believe that notice-triggering information was acquired by an unauthorized person, implement your notification plan.

1. Notify California residents whose notice-triggering information was acquired by an unauthorized person.
2. Notify affected individuals in situations involving unauthorized acquisition of notice-triggering information in any format, including computer printouts and other paper records.
3. If you cannot identify the specific individuals whose notice-triggering information was acquired, notify all those in the groups likely to have been affected,

such as all whose information is stored in the files involved.

4. Avoid false positives. A false positive occurs when the required notice of a security breach is sent to individuals who should not receive it because their personal information was not acquired as part of the breach. Consider the following when identifying the group that will be notified.
   - Before sending individual notices, make reasonable efforts to include only those individuals whose notice-triggering information was acquired.
   - Implement procedures for determining who gets included in the notice and who does not. Check the mailing list before sending the notice to be sure it is not over-inclusive.
   - Document your process for determining inclusion in the group to be notified.

Contact Credit Reporting Agencies on Large Breaches of Financial-Related Information

A breach involving a large number of individuals can potentially have a significant impact on consumer reporting agencies and their ability to respond efficiently. High volumes of calls could impede access to the agencies. Be sure to contact the agencies before you send out notices in cases involving a large number of individuals - 10,000 or more. Note that this step is relevant for breaches of Social Security numbers, driver's license or California ID numbers, or financial account numbers - not for breaches of medical or health insurance information alone.

1. Make arrangements with the credit reporting agencies during your preparations for giving notice, without delaying the notice for this reason.
2. Organizations should contact the consumer credit reporting agencies as follows.
   - Experian: Send an e-mail to BusinessRecordVictimAssistance @Experian.com.
   - Equifax: Send an e-mail to businessrecordsecurity@equifax.com.
   - TransUnion: Send an e-mail to fvad@transunion.com, with "Database Compromise" as the subject.

Contents of Notice

A sample notice letter is attached as Appendix 2. Include the following information in your notice to affected individuals:

1. A general description of what happened.
2. The specific type of personal information that was involved.
   - In breaches of financial-related information, specify whether Social Security number, driver's license or California ID number, or financial account number was involved.
   - In breaches of medical or health insurance information, be as specific as possible about the nature of the information involved. Specify that Social Security numbers, driver's license numbers and financial account numbers were not involved, when that is the case.
3. What you have done to protect the individual's personal information from further unauthorized acquisition.
4. What your organization will do to assist individuals, including providing your toll-free contact telephone number for more information and assistance.
5. Information on what individuals can do to protect themselves from identity theft, as appropriate for the specific type of personal information involved.
   - See the sample notice letter in Appendix 2. Note that this sample letter is intended for California residents. The information

on contacting DMV, for example, does not apply to other states.

6. Contact information for the Web site of the California Office of Privacy Protection (www.privacy.ca.gov) for additional information for California residents on protection against identity theft.

Form and Style of Notice

Make the notice clear, conspicuous and helpful.

1. Use clear, simple language, guiding subheads, and plenty of white space in the layout.
2. Avoid jargon or technical language.
3. Avoid using a standardized format, which could result in making the public complacent about the process and thus undercut the purpose of the notice.

Means of Notification

Individually notify those affected whenever possible.

1. Send the notice by first-class mail.
2. As an alternative, notify by e-mail, if you normally communicate with the affected individuals by e-mail and you have received their prior consent to that form of notification.
3. If more than 500,000 individuals were affected, the cost of individual notification is more than $250,000, or you do not have adequate contact information on those affected, provide notice using public communication channels.
    - Post the notice conspicuously on your Web site, AND
    - Notify through major statewide media (television, radio, print), AND
    - Send the notice by e-mail to any affected party whose e-mail adddress

Notes

you have.

[1]Javelin Strategy & Research's "2008 Identity Fraud Survey Report," published February 2008. An abbreviated version is available for free and the full survey reports may be purchased online at www.javelinstrategy.com.

[2]According to the data in the 2008 Javelin survey report cited above, 65% of the victims surveyed did not know how their information was acquired by identity thieves. In addition, 20% said their information was in lost or stolen mail, wallet, or credit card; 8% said it was stolen during a transaction; 4% online; 2% in a data breach; and 1% other.

[3]"Identity Theft: Predator Profiles," Collins, J.M. and Hoffman, S.K. (2004). Available from Judith Collins, School of Criminal Justice, Michigan State University.

[4]The World Privacy Forum's research on medical identity theft is available at www.worldprivacyforum.org.

[5]This formulation of the security safeguards principle is from the Organisation for Economic Cooperation and Development (OECD)'s *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, available at www.oecd.org. The U.S. participated in the development of these principles and reaffirmed their viability as recently as 1998, in the *Declaration on the Protection of Privacy in Global Networks*. In that work, the U.S. committed to respecting individual privacy rights as an essential component to building and retaining public confidence in a marketplace that is increasingly global and increasingly online. The Principles form the foundation of most privacy laws in the U.S. and elsewhere.

[6]The Gramm-Leach-Bliley Act, 15 U.S.C 6801-6827, includes the Safeguards Rule, "Standards for Insuring the Security, Confidentiality, Integrity and Protection of Customer Records and Information," 16 C.F.R. Part 314. The Health Insurance Portability and Accountability Act, PL 104-191, includes "Health Insurance Reform: Security Standards," 45 C.F.R. Parts 160, 162, and 164.

[7]California Civil Code § 1798.81.5 requires companies that collect specified personal information (name plus Social Security number, driver's license or state ID number, financial account number, or medical information) on California residents to use reasonable and appropriate security safeguards to protect it. It also requires such companies to contractually obligate service providers to the same standards.

[8]California Civil Code § 1798.21. The Information Practices Act, Civil Code § 1798 et seq., imposes specific responsibilities for protecting the security and confidentiality of records containing personal information.

[9]The Privacy Rights Clearinghouse maintains a list of publicly known breach notifications at www.privacyrights.org. While this list does not represent all breaches or even all notifications, it is the most comprehensive list available.

[10]In a May 2008 revew of 880 breach notifications on the Privacy Rights Clearinghouse list cited above, 45% of the incidents resulted from a lost or stolen computer, thumb drive, back-up tape or other medium. Eighteen percent were due to hacking, 14% to inadvertant Web exposure, 6% to improper disposal, 5% to insider fraud, and the remaining 12% to mailing or emailing errors, lost mail, and other causes.

[11]California Government Code § 11549.5(a).

[12]California Government Code § 11549.5(c).

[13]The internationally recognized information security standard is ISO/IEC 27001, a comprehensive set of controls comprising best practices in information security. For more information on the principles and practices of information security, see Appendix 5: Information Security Resources.

[14]The State of California has adopted a policy requiring State agencies to encrypt "notice-triggering" and medical information on portable computing devices or portable storage media. See BL05-32, available on the Policy page at www.infosecurity.ca.gov.

[15]See California Civil Code § 1798.81.5.

[16]Effective May 26, 2002, the encryption standard approved for U.S. Government organizations and others to protect higher-risk information is FIPS 197. For more information, see http://csrc.nist.gov/publications/PubsFIPS.html .

[17]See Special Publication 800-88, *Guidelines for Media Sanitization*, published in February 2006 by the Computer Security Division of the National Institute of Standards and Technology, available at http://csrc.nist.gov/publications/PubsSPs.html.

[18]ISO/IEC 27001, cited in note 14 above, includes practices related to responding to and reporting security incidents and malfunctions "as quickly as possible" (§ 6.3).

[19]See Appendix 4 for suggestions on computer security incident response from the California Highway Patrol's Computer Crimes Investigations Unit and the FBI's National Computer Crime Squad.

[20]15 U.S. Code § 7001 contains the requirements for consumer disclosure and consent to electronic notification, as required by California Civil Code §§ 1798.29(g)(2) and 1798.82(g)(2).

Appendix 1: Advisory Group

2003 Original Version

The following people provided consultation and advice to the California Office of Privacy Protection in the development of the original version of these Recommended Practices, issued in Ocotber 2003.

Brent Barnhart
Senior Counsel
Kaiser Foundation Health Plan, Inc.

Camille Busette
Senior Policy Manager
Intuit

Dianne Carpenter
Senior Attorney
J.C. Penney Corporation
California Retailers Association

James Clark
Senior Vice President
Government Relations
California Bankers Association

Mari Frank
Attorney, Privacy Consultant, and Author

Beth Givens
Director
Privacy Rights Clearinghouse

Roxanne Gould
Vice President,
CA Public and Legislative Affairs
American Electronics Association

Chief Kevin Green
California Highway Patrol

Craig Grivette
Deputy Secretary
California Business,
Transportation and Housing Agency

Tony Hadley
Vice President
Government Affairs
Experian

Gail Hillebrand
Senior Attorney
Consumers Union

Clark Kelso
Chief Information Officer
State of California

Barbara Lawler
Chief Privacy Officer
Hewlett-Packard

Fran Maier
Executive Director
TRUSTe

Dana Mitchell
Counsel to Rules Committee
California State Senate

Peter Neumann
Principal Scientist
Computer Science Lab
SRI International

Dr. Larry Ponemon
Chairman
Ponemon Institute

Debra Reiger
Chief Information Security Officer
State of California

Tim Shea
Legal Counsel
California Franchise Tax Board

Scott Shipman
Privacy Counsel
eBay

Preston Taylor
Consultant to
Assemblyman Joseph Simitian
California State Assembly

Tracey Thomas
Identity Theft Resource Center

Tom Timmons
President & CEO, Spectrum Bank
California Independent Bankers

2008 Revision

The Office of Privacy Protection was assisted in the May 2008 revision by advice from the following people.

Linda Ackerman
Staff Counsel
Privacy Activisim

Sharon Anolik
Director, Corporate Compliance and Ethics
Chief Privacy Officer
Blue Shield of California

Pam Dixon
Executive Director
World Privacy Forum

Mari Frank
Attorney, Privacy Consultant and Author

Beth Givens
Director
Privacy Rights Clearinghouse

Robert Herrell
Legislative Director
Assembly Member Dave Jones

Reece Hirsch
Sonnenschein, Nath & Rosenthal

Bobbie Holm
Chief, Policy Branch
California Office of HIPAA Implementation

Chris Hoofnagle
Senior Staff Attorney
Samuelson Law, Technology & Public Policy Clinic

Edward Howard
Howard Advocacy Inc.
for American Electronics Association

Dr. Rory Jaffe
Executive Director, Medical Services
University of California Office of the President

Saskia Kim
Principal Consultant
Senate Office of Research

Valerie Nera
Policy Advocate
California Chamber of Commerce

Lori Potter
Counsel, Legal and Government Relations
Kaiser Foundation Health Plan, Inc.

Appendix 2: Sample Notice Letter

Dear :

We are writing to you because of a recent incident at [*name of organization*]. *Describe what happened in general terms, specifically what kind of personal information was involved, and what you are doing in response.*

Tell people what to do to protect themselves. What actions to recommend will depend on the type of information involved, in addition to name. Use the information from one or more on the following sections.

Social Security Number

Because your Social Security number was involved, we recommend that you place a fraud alert on your credit files. A fraud alert requires potential creditors to use what the law refers to as "reasonable policies and procedures" to verify your identity before issuing credit in your name. A fraud alert lasts for 90 days. Just call one of the three credit reporting agencies at a number below. This will let you automatically place an alert with all of the agencies. You will receive letters from all three, confirming the fraud alert and letting you know how to get a free copy of your credit report from each.

Experian 1-888-397-3742 Equifax 1-800-525-6285 TransUnion 1-800-680-7289

When you receive your credit reports, look them over carefully. Look for accounts you did not open. Look for inquiries from creditors that you did not initiate. And look for personal information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

If you do find suspicious activity on your credit reports, call your local police or sheriff's office and file a police report of identity theft. [*If appropriate, also give the contact number for the law enforcement agency investigating the incident for you.]* Get a copy of the police report. You may need to give copies of the police report to creditors to clear up your records.

Even if you do not find any signs of fraud on your reports, we recommend that you check your credit reports periodically. You can keep the fraud alert in place by calling again after 90 days. For more information on identity theft, we suggest that you visit the web site of the California Office of Privacy Protection at www.privacy.ca.gov.

If there is anything that [*name of organization*] can do to assist you, please call us at [*toll-free phone number*].

California Driver's License or Identification Card Number

Since your California driver's license [or California Identification Card] number was involved, we recommend that you call the DMV Fraud Hotline at 1-866-658-5758 to report it.

Continue with above advice for Social Security numbers.

Financial Account Number

To protect yourself from the possibility of identity theft., we recommend that you immediately

contact [*credit card or financial account issuer*] at [*phone number*] and close your account. Tell them that your account may have been compromised, and ask that they report it as "closed at customer request." If you want to open a new account, ask [*name of account issuer*] to give you a PIN or password. This will help control access to the account.

For more information on identity theft, we suggest that you visit the web site of the California Office of Privacy Protection at www.privacy.ca.gov.

If there is anything that [*name of organization*] can do to assist you, please call us at [*toll-free phone number*].

Medical Information or Health insurance Information (as defined)

If the breach does not include Social Security, driver's license/California Identification Card, or financial account numbers, say so. If it does include any of those numbers in addition to medical or health insurance information, then also include the information on what to do from the appropriate section(s) above.

We recommend that you regularly review the explanation of benefits statement that you receive from [*us, your plan, your insurer*]. If you see any service that you believe you did not receive, please contact [*us, your plan, your insurer*] at the number on the statement [*or provide a number here*]. If you do not receive regular explanation of benefits statements, contact your provider or plan and request them to send such statements following the provision of services in your name or number.

You may want to order copies of your credit reports and check for any medical bills that you do not recognize. If you find anything suspicious, call the credit reporting agency at the phone number on the report. You can order your reports from the three credit reporting agencies for free each year by calling 1-877-322-8228 or going to www.annualcreditreport.com.

Keep a copy of this notice for your records in case of future problems with your medical records. You may also want to request a copy of your medical records from [*your provider or plan*], to serve as a baseline. For information on your medical privacy rights, we suggest that you visit the web site of the California Office of Privacy Protection at www.privacy.ca.gov.

If there is anything that [*name of organization*] can do to assist you, please call us at [*toll-free number*].

Appendix 3: California Law on Notice of Security Breach

Summary of Breach Notice Law

California Civil Code Section 1798.29 applies to state government agencies and Sections 1798.82 and 1798.84 apply to any person or business doing business in California. The main provisions are summarized below.

Security Breach

- Unauthorized acquisition of computerized data that compromises the security, confidentiality or integrity of personal information.

Type of Information

- Unencrypted computerized data including certain personal information.
- Personal information that triggers the notice requirement is name (first name or initial and last name) plus any of the following:
  - Social Security number,
  - Driver's license or California Identification Card number,
  - Financial account number, credit or debit card number (along with any PIN or other access code where required for access to account),
  - Medical information, as defined, or
  - Health insurance information, as defined.

Whom to Notify

- Notice must be given to any data subjects who are California residents.

When to Notify

- Timing: "in the most expedient time ossible and without unreasonable delay." Time may be allowed for the following:
  - Legitimate needs of law enforcement if notification would impede a criminal investigation.
  - Taking necessary measures to determine the scope of the breach and restore reasonable integrity to the system.

How to Notify

- Notice may be provided in writing, electronically (as consistent with provisions of 15 U.S. Code 7001), or by substitute notice.
- Substitute notice may be used if the cost of providing individual notice is more than $250,000, more than 500,000 people would have to be notified, or the organization does not have sufficent contact information for those affected.
- Substitute notice means all of the following:
  - E-mail when the e-mail address is available, AND
  - Conspicuous posting on Web site, AND
  - Notification of major statewide media.
- Alternatively, a business or agency may use its own notification procedures as part of an information security policy, if its procedures are consistent with the timing requirements of the law and if it notifies subjects in accordance with its policy.

Text of California Civil Code Sections 1798.29, 1798.82, and 1798.84

1798.29. (a) Any agency that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(b) Any agency that maintains computerized data that includes personal information that the agency does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(c) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.

(d) For purposes of this section, "breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the agency. Good faith acquisition of personal information by an employee or agent of the agency for the purposes of the agency is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

(e) For purposes of this section, "personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

(1) Social security number.

(2) Driver's license number or California Identification Card number.

(3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

(4)Medical information.

(5) Health insurance information.

(f) (1) For purposes of this section, "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(2) For purposes of this section, "medical information" means any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional.

(3) For purposes of this section, "health insurance information" means an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify athe individual, or any information in an individual's applicaton and claims history, including any appeals records.

(g) For purposes of this section, "notice" may be provided by one of the following methods:

(1) Written notice.

(2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code.

(3) Substitute notice, if the agency demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars ($250,000), or that the affected class of subject persons to be notified exceeds 500,000, or the agency does not have sufficient contact information. Substitute notice shall consist of all of the following:

(A) E-mail notice when the agency has an e-mail address for the subject persons.

(B) Conspicuous posting of the notice on

the agency's Web site page, if the agency maintains one.

(C) Notification to major statewide media.

(h) Notwithstanding subdivision (g), an agency that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this part shall be deemed to be in compliance with the notification requirements of this section if it notifies subject persons in accordance with its policies in the event of a breach of security of the system.

1798.82. (a) Any person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(b) Any person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(c) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.

(d) For purposes of this section, "breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

(e) For purposes of this section, "personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

(1) Social security number.

(2) Driver's license number or California Identification Card number.

(3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

(4)Medical information.

(5) Health insurance information.

(f) (1) For purposes of this section, "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(2) For purposes of this section, "medical information" means any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional.

(3) For purposes of this section, "health insurance information" means an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify athe individual, or any information in an individual's applicaton and claims history, including any appeals records.

(g) For purposes of this section, "notice" may be provided by one of the following methods:

(1) Written notice.

(2) Electronic notice, if the notice provided

is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code.

(3) Substitute notice, if the person or business demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars ($250,000), or that the affected class of subject persons to be notified exceeds 500,000, or the person or business does not have sufficient contact information. Substitute notice shall consist of all of the following:

(A) E-mail notice when the person or business has an e-mail address for the subject persons.

(B) Conspicuous posting of the notice on the Web site page of the person or business, if the person or business maintains one.

(C) Notification to major statewide media.

(h) Notwithstanding subdivision (g), a person or business that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this part, shall be deemed to be in compliance with the notification requirements of this section if the person or business notifies subject persons in accordance with its policies in the event of a breach of security of the system.

1798.84. (a) Any waiver of a provision of this title is contrary to public policy and is void and unenforceable. (b) Any customer injured by a violation of this title may institute a civil action to recover damages. (c) In addition, for a willful, intentional, or reckless violation of Section 1798.83, a customer may recover a civil penalty not to exceed three thousand dollars ($3,000) per violation; otherwise, the customer may recover a civil penalty of up to five hundred dollars ($500) per violation for a violation of Section 1798.83.

(d) Unless the violation is willful, intentional, or reckless, a business that is alleged to have not provided all the information required by subdivision (a) of Section 1798.83, to have provided inaccurate information, failed to provide any of the information required by subdivision (a) of Section 1798.83, or failed to provide information in the time period required by subdivision (b) of Section 1798.83, may assert as a complete defense in any action in law or equity that it thereafter provided regarding the information that was alleged to be untimely, all the information, or accurate information, to all customers who were provided incomplete or inaccurate information, respectively, within 90 days of the date the business knew that it had failed to provide the information, timely information, all the information, or the accurate information, respectively.

(e) Any business that violates, proposes to violate, or has violated this title may be enjoined.

(f) A prevailing plaintiff in any action commenced under Section 1798.83 shall also be entitled to recover his or her reasonable attorney's fees and costs.

(g) The rights and remedies available under this section are cumulative to each other and to any other rights and remedies available under law.

Appendix 4: Reporting to Law Enforcement

Law Enforcement Contacts for Computer Crimes

California High Technology Theft and Apprehension Program
This program funds five regional task forces staffed by investigators from local, state and federal law enforcement agencies who have received specialized training in the investigation of high technology crime and identity theft investigations. High technology crimes are those crimes in which technology is used as an instrument in committing, or assisting in the commission of, a crime, or is the target of a criminal act.

Sacramento Valley Hi-Tech Crimes Task Force
Telephone: 916-874-3002
www.sachitechcops.org

Southern California High Tech Task Force
Telephone: 562-347-2601

Northern California Computer Crimes Task Force
Telephone: 707-253-4500
www.nc3tf.org

Rapid Enforcement Allied Computer Team (REACT)
Telephone: 408-494-7186
http://reacttf.org

Computer and Technology Crime High-Tech Response Team (CATCH)
Telephone: 619-531-3660
http://www.catchteam.org/

FBI
Local Office: http://www.fbi.gov/contact/fo/fo.htm
National Computer Crime Squad
Telephone: 202-324-9164
E-mail: nccs@fbi.gov
www.emergency.com/fbi-nccs.htm

U.S. Secret Service
Local Office: www.treas.gov/usss/index.shtml
Cyber Threat/Network Incident Report: www.treas.gov/usss/net_intrusion_forms.shtml

Procedures the Computer User Should Institute Both Prior to Becoming a Computer Crime Victim and After a Violation Has Occurred

Guidance from the FBI National Computer Crime Squad
www.emergency.com/fbi-nccs.htm

- Place a login banner to ensure that unauthorized users are warned that they may be subject to monitoring.
- Turn audit trails on.
- Consider keystroke level monitoring if adequate banner is displayed.
- Request trap and tracing from your local telephone company.
- Consider installing caller identification.
- Make backups of damaged or altered files.
- Maintain old backups to show the status of the original.
- Designate one person to secure potential evidence
- Evidence can consist of tape backups and printouts. These should be initialed by the person obtaining the evidence. Evidence should be retained in a locked cabinet with access limited to one person.
- Keep a record of resources used to reestablish the system and locate the perpetrator.

Reporting a Computer Crime to Law Enforcement

Guidance from the California Highway Patrol Computer Crimes Investigation Unit
www.chp.ca.gov/programs/ccrime-incident.html#do

When reporting a computer crime be prepared to provide the following information:

- Name and address of the reporting agency.
- Name, address, e-mail address, and phone number(s) of the reporting person.
- Name, address, e-mail address, and phone number(s) of the Information Security Officer (ISO).
- Name, address, e-mail address, and phone number(s) of the alternate contact (e.g., alternate ISO, system administrator, etc.).
- Description of the incident.
- Date and time the incident occurred.
- Date and time the incident was discovered.
- Make/model of the affected computer(s).
- IP address of the affected computer(s).
- Assigned name of the affected computer(s).

- Operating System of the affected computer(s).
- Location of the affected computer(s).

Incident Response DOs and DON'Ts

DOs

1. Immediately isolate the affected system to prevent further intrusion, release of data, damage, etc.
2. Use the telephone to communicate. Attackers may be capable of monitoring E-mail traffic.
3. Immediately notify an appropriate law enforcement agency.
4. Activate all auditing software, if not already activated.
5. Preserve all pertinent system logs, e.g., firewall, router, and intrusion detection system.
6. Make backup copies of damaged or altered files, and keep these backups in a secure location.
7. Identify where the affected system resides within the network topology.
8. Identify all systems and agencies that connect to the affected system.
9. Identify the programs and processes that operate on the affected system(s), the impact of the disruption, and the maximum allowable outage time.
10. In the event the affected system is collected as evidence, make arrangements to provide for the continuity of services, i.e., prepare redundant system and obtain data back-ups. To assist with your operational recovery of the affected system(s), pre-identify the associated IP address, MAC address, Switch Port location, ports and services required, physical location of system(s), the OS, OS version, patch history, safe shut down process, and system administrator or backup.

DON'Ts

1. Delete, move, or alter files on the affected systems.
2. Contact the suspected perpetrator.
3. Conduct a forensic analysis.

California Penal Code Definition of "Computer Crime"[1]

As defined by California Penal Code Section 502, subsection (c), a computer crime occurs when a person:

(1) Knowingly accesses and without permission alters, damages, deletes, destroys, or otherwise uses any data, computer, computer system, or computer network in order to either (A) devise or execute any scheme or artifice to defraud, deceive, or extort, or (B) wrongfully control or obtain money, property, or data.

(2) Knowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting docu-

mentation, whether existing or residing internal or external to a computer, computer system, or computer network.

(3) Knowingly and without permission uses or causes to be used computer services.

(4) Knowingly accesses and without permission adds, alters, damages, deletes, or destroys any data, computer software, or computer programs which reside or exist internal or external to a computer, computer system, or computer network.

(5) Knowingly and without permission disrupts or causes the disruption of computer services or denies or causes the denial of computer services to an authorized user of a computer, computer system, or computer network.

(6) Knowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or computer network in violation of this section.

(7) Knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network.

(8) Knowingly introduces any computer contaminant into any computer, computer system, or computer network.

(9) Knowingly and without permission uses the Internet domain name of another individual, corporation, or entity in connection with the sending of one or more electronic mail messages, and thereby damages or causes damage to a computer, computer system, or computer network.

[1]Other violations of California or federal law may also be involved in an incident of unauthorized acquisition of personal information. California laws that may be involved include identity theft (Penal Code § 530.5), theft (Penal Code § 484), or forgery (Penal Code § 470).

Appendix 5: Information Security Resources

Federal Trade Commission, "Financial Institutions and Customer Data: Complying with the Safeguards Rule," available at www.ftc.gov/bcp/conline/pubs/buspubs/safeguards.htm.

Federal Trade Commission, "Security Check: Reducing Risks to Your Computer Systems," available at www.ftc.gov/bcp/conline/pubs/buspubs/security.htm.

"Health Insurance Reform: Security Standards; Final Rule," 45 CFR Parts 160, 162 and 164, available at www.cms.hhs.gov/hipaa/hipaa2/regulations/security/default.asp.

ISO/IEC 27001, Information Technology - Security Techniques - Information Security Management systems - Requirements, available at www.iso.org.

ISO/IEC 27002, Information Technology - Security Techniques - Code of Practice for Information Security Management, available at www.iso.org.

National Institute for Standards and Technology (NIST) Computer Security Resource Center, available at www.csrc.nist.gov.

Payment Card Industry Data Security Standard, available at www.visa.ca/ais and https://sdp.mastercardintl.com.

SANS, "Top 20 Security Risks" (updated annually) and "Best Practices for Preventing Top 20 Risks", available at www.sans.org/top20/.

U.S. CERT, Cyber Security Tips, available at www.uscert.gov/cas/tips/index.html.

California Office of Privacy Protection
www.privacy.ca.gov

Office of Information Security & Privacy Protection
www.oispp.ca.gov

State and Consumer Services Agency
www.scsa.ca.gov